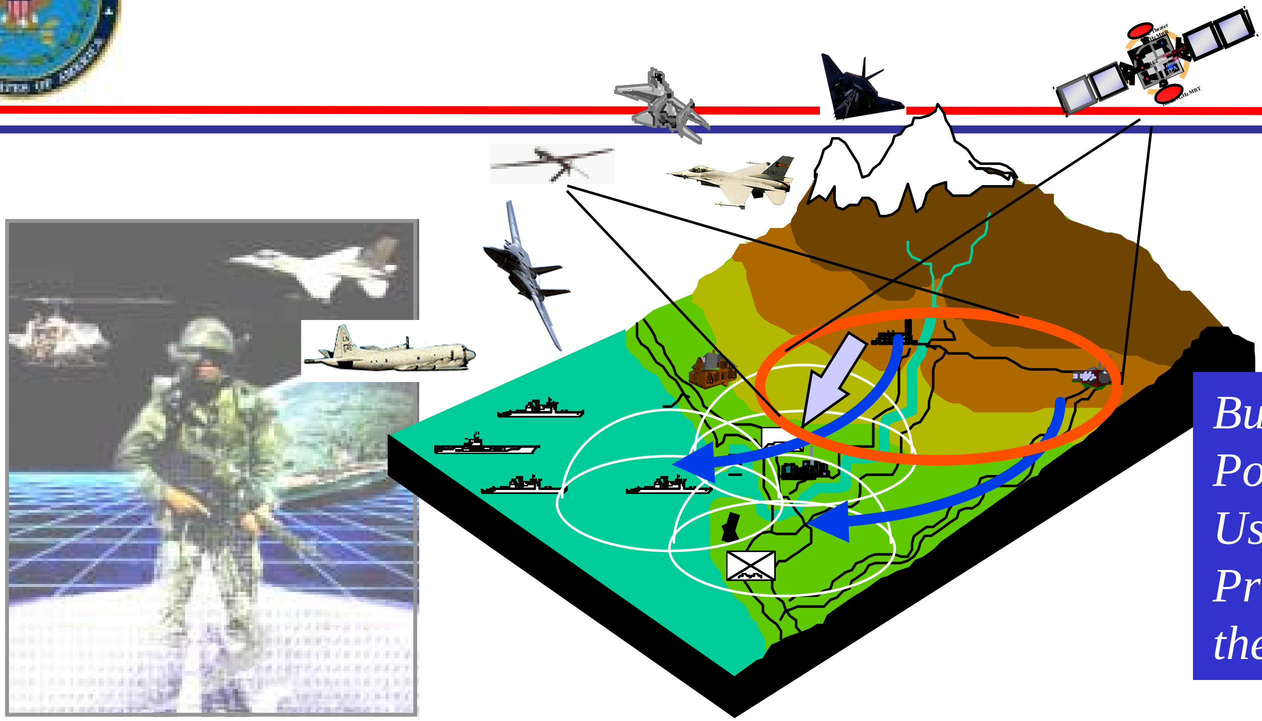

Build…
Populate…
Use…&…
Protect…
the Network

DoD Wireless Policy Development: Status Brief

Federal Wireless Users Forum Group
May 2002

Executive Summary

- Current and emerging wireless technologies offer many convenient applications - Wireless email, PDAs, WLANs, etc
- With the growing use of wireless capabilities comes an increased awareness of vulnerabilities and risks that must be managed
- NSA Information Systems Security Organization issued Information Assurance Advisory, Jan 2001 Subject: Personal Electronic Devices Security Guidance
- Services followed with various policy initiatives on Wireless LANs, PDAs, and Wireless email systems
- Air Force/SC memo to ASD(C3I) requested OASD (C3I) establish a working group to develop an overarching wireless policy for the Global Information Grid
- Four "roll up sleeves" working group meetings (S/D/A/JS/Labs, etc.)
- Five iterations of the draft policy yielded hundreds of comments (solicited and unsolicited) from both government and industry individuals
- Draft policy ready for SD106 coordination (Approximately 3 months)

Near Term Objectives
(Working Group Focus)

- Develop an overarching wireless policy to guide management and use of current & evolving Wireless Local Area Network (LAN) technologies and Portable Electronic Devices (PEDs) systems
  - Sufficiently flexible to allow implementation of Service unique capabilities
  - Policy pillars to include (as a minimum): Security; Interoperability; Technology; Spectrum
- Balance benefits of wireless functionality and managing security risks
- Set stage to better integrate future technologies (e.g., Ultra wideband) into policy

Note: PEDs include Two-way Pagers, Personal Digital Assistants, Palmtops, Handheld computers, cell phones/PCS, keyboards, scanners etc.

Our Starting Point

(DoD Wireless Conference July 10-11, 2001)

- Objective to provide a forum to exchange information on:
  - Operational use, implementation plans, current/planned pilots, extant/evolving policies, spectrum concerns and security implications associated with the use of wireless in DoD
  - Use information to assist in building the foundation for the overarching DoD wireless policy
- Over 90 attendees representing wide range of OSD, Joint Staff, Services, and Agencies, Laboratory offices
- Presentations provided on:
  - OSD activities (C3I and AT&L)
  - Wireless vulnerability issues and assessments (NSA and Air Force)
  - Service/Department pilots/policy/implementation plans (All services and DISA)
- Excellent exchange - many participants discussed the benefits and attendant risks/concerns involved in use of wireless devices
- "Roundtable" feedback provided at end of conference
- First Wireless Policy Working Group convened

Preliminary Policy Development Recommendations

(Derived From the Conference/First Working Group Meeting)

- Strike a balance between the benefits using wireless devices and managing the associated security risks
- Be consistent with current DoD policy
- Be general enough to cover all wireless devices, including future devices
  - Provide local authorities freedom to formulate local specific requirements, vulnerability assessments, and guidelines
- Structure policy to enhance interoperability
- In addition to security and interoperability, address requirements, threat, standards, spectrum and technology
- Policy should be simple and user friendly
  - utilize a web site and fast jump capability to obtain guidelines on use of a specific device

What is a DoD Directive?

- Governed by DoDD 5025.1-M (Aug. 1994) - DoD Directive System
- Approved and signed by the SECDEF or DSECDEF
- Used for centralized policy-making
  - – provide policy guidance
  - – fixing responsibility
  - – establishing mechanisms for feedback and oversight
- DoD Components provided the latitude to determine how a policy is to be implemented at the local level
- Format
  - – should* be streamlined into six pages or less
  - – no procedures - “when procedures are necessary to carry out or support DoD policy, Instructions or Publications should be issued”
- Director of Administration and Management, Office of SECDEF coordinates ALL proposed DoD issuances

***** Should - Action is required, unless justifiable reason exists for not taking action.

Directive Outline

(Pre-coordination Draft)

- 1. PURPOSE..
- 2. APPLICABILITY AND SCOPE
- 3. DEFINITIONS
- 4. POLICY
- 5. RESPONSIBILITIES
- 6. EFFECTIVE DATE

- E1. ENCLOSURE 1: DEFINITIONS
- E2. ENCLOSURE 2: REFERENCES
- E3. ENCLOSURE 3: MITIGATING ACTIONS AGAINST WIRELESS SYSTEM VULNERABILITIES

Policy Overview

(Pre-coordination Draft)

- Applies to all wireless devices, both as part of the GIG and as stand-alone
- “Raise the awareness” of users to policies already in place
- Establishes minimum thresholds
- Empowers DAAs to assess local implementations
- Establishes Knowledge Management Process to share information across the enterprise
- Promotes Joint Interoperability

Section 4 - Policy (Draft)

(The Empowering of the DAAs)

- NSA-approved Type-1 end-to-end encryption will be utilized for CLASSIFIED information
- Federal Information Processing Standards (FIPS) 140-1/2 encryption will be used for UNCLASSIFIED information. DAA is authorized to grant individual exceptions on a case-by-case basis.
- DoD Public Key Infrastructure (PKI) will be used for Identification and Authentication (I&A)
- Wireless devices shall not be permitted inside a permanent, temporary, or mobile Sensitive Compartmented Information Facility (SCIF)
- The DITSCAP will be used to assess the overall security architecture of wireless devices and the networks they operate with
- The cognizant DAA shall govern the use of wireless devices
  - Wireless devices shall not be connected to DoD systems without the approval of the cognizant DAA.
  - DoD-controlled wireless devices shall not be connected to non-DoD systems without the approval of the cognizant DAA.
  - Personally owned wireless devices shall not be connected to DoD information systems without the approval of the cognizant DAA.
  - Reaccredit IS operations upon introduction of wireless technologies
- Joint and Combined Interoperability
  - Based on Standards
  - Spectrum management
- Develop, implement and oversee Knowledge Management process

Policy Provides IA-Related Details

(Pre-coordination Draft)

- **Classified Information**
  - Must use Type-One encryption
  - Must have DAA approval
  - Must use PKI for Identification & Authentication
- **Unclassified Information**
  - Must use, as a minimum, FIPS 140-1/2 encryption
    - Can be waived by DAA on case-by-case basis
  - Must use PKI for I&A
- **Other**
  - Wireless devices are not allowed to operate in SCIFs
  - DAA approves use of wireless in “classified” areas
  - Enclosure contains mitigating actions against wireless system vulnerabilities

Policy Excerpts

(Pre-coordination Draft)

- **Classified Information**
  - 4.2.1. Wireless technologies/devices shall not be used for storing, processing, and/or transmitting CLASSIFIED information without explicit approval of the DAA in accordance with reference (e).
  - 4.2.2. Wireless devices that transmit CLASSIFIED information, over a network, shall use the DoD Public Key Infrastructure (PKI) high assurance mechanisms for Identification and Authentication (I&A) in accordance with reference (d).
  - 4.2.3. Only assured channels employing NSA-approved, Type-1 end-to-end encryption shall be used to transmit classified information.
  - 4.2.4. The storage of CLASSIFIED information on PEDS requires the information to be encrypted using NSA approved, Type-1 encryption software and techniques.

Policy Excerpts (Continued -1)

(Pre-coordination Draft)

- **Unclassified Information**
  - 4.1.2. Confidentiality. Encryption of unclassified information for transmission to and from wireless devices is required. The DAA is authorized to grant individual exceptions on a case-by-case basis...
    - 4.1.2.1. Data. Encryption must be implemented end-to-end over an assured channel and shall meet the FIPS 140-1 or 2, Overall Level 2 ((Triple-DES or AES) standard (reference (f&g)), at a minimum...
    - 4.1.2.2. Voice. Voice does not require encryption unless used to access a voice recognition / synthesis driven data application (e.g., VoiceXML).
  - 4.1.1. Identification and Authentication (I&A). Strong authentication, non-repudiation, and personal identification is required for access to DoD IS in accordance with DoD PKI policy (reference (d)). I&A measures shall be implemented at both the device and network level.

Policy Excerpts (Continued -2)

(Pre-coordination Draft)

- **Other**
- 4.1.3. Data Integrity. Wireless devices that store and process information often do not have the same degree of protection afforded by standard desktop operating and file management systems. The DAA shall require wireless devices to implement file system encryption (where applicable)…
- 4.3. Wireless devices shall not be operated inside a permanent, temporary, or mobile Sensitive Compartmented Information Facility (SCIF) in accordance with chapter 15 of Joint DoD/IIS Cryptologic SCI Systems Security Standards.
- 4.4. Wireless technologies/devices used for storing, processing, and/or transmitting UNCLASSIFIED information shall not be used in areas where CLASSIFIED information is stored, processed, or transmitted unless a minimum separation distance is maintained between the UNCLASSIFIED wireless processing device and the CLASSIFIED processing device as determined by the DAA.

Enclosure 3 Excerpts (Mitigating actions against vulnerabilities)

(Pre-coordination Draft)

- **PANs**
  - E3.1.2. PAN technologies shall not be utilized for transmitting UNCLASSIFIED information unless the data is encrypted per Section 4.1.
- **WLANs**
  - E3.2.2. WLAN technologies shall not be utilized for transmitting UNCLASSIFIED information unless the data is encrypted per Section 4.1
- **PEDs**
  - E3.5.2.1. Therefore PEDs that are connected directly to a DoD wired network (e.g., via a hot synch connection to a workstation) shall not be permitted to operate wirelessly at the same time.

Summary

- Policy development:
  - Continues to be high interest item
  - Excellent participation
  - Maintained balance between functionality and security
  - Extensive pre-coordination phase completed
  - About to enter formal SD106 process
- Expected three month coordination

Questions?

Contact Information:

Mr. Carl Consumano

Office of the DoD CIO

703-607-0477

carl.consumano@osd.mil

carl.consumano@osd.smil.mil